

INCIDENT RESPONSE NOTIFICATION SYSTEM

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] The present disclosure claims the benefit of U.S. Provisional Patent Application No.: 63/450,487 filed on 2023-03-07, the entirety of which is incorporated herein by reference.

FIELD

[0002] The present disclosure is generally related to coordination among sensors, and more particularly to organizing signals received from wirelessly deployed sensors into a coherent action plan accessible to a plurality of users for incidents indented by several sensors, individually or in tandem.

SUMMARY

[0003] The present disclosure provides an incident response notification system using wirelessly deployed sensors communicated to and coordinate through a central service, which is accessible by a plurality of users. The locations of these sensors are known to the central service, so that when a sensor generates an alert or other report, the central service can track the various events monitored by the sensors across time and space. By amalgamating the reports from several sensors, the central service can identify trends in events (e.g., a flow of events) to provide one or more users with relevant alerts, reaction plans based on the flow of events, and predictions for future events in the flow of events. Accordingly, the present disclosure provides an improved user experience and additional functionality for various sensors and the users of those sensors.

[0004] Additional features and advantages of the disclosed method and apparatus are described in, and will be apparent from, the following Detailed Description and the Figures. The features and advantages described herein are not all-inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the figures and description. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes, and not to limit the scope of the inventive subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figure 1 illustrates an operations environment for an incident response notification system, according to embodiments of the present disclosure.

[0006] Figure 2 is a flowchart for an example method of deploying an incident response notification system, according to embodiments of the present disclosure.

[0007] Figure 3 is a flowchart for an example method of operating an incident response notification system, according to embodiments of the present disclosure.

[0008] Figure 4 is a time chart of operating an incident response notification system, according to embodiments of the present disclosure.

[0009] Figure 5 is a flowchart of an example incident response, according to embodiments of the present disclosure.

[0010] Figure 6A illustrates a computing device, according to embodiments of the present disclosure.

[0011] Figures 6B-6C illustrate examples of various sensors and input/output devices as may be included in or in communication with various computing devices, according to embodiments of the present disclosure.

[0012] Figure 7A illustrates an example of a hybrid peer-to-peer (P2P) computing model, according to embodiments of the present disclosure.

[0013] Figure 7B illustrates an example of a structured P2P computing model, according to embodiments of the present disclosure.

DETAILED DESCRIPTION

[0014] The present disclosure provides an incident response notification system using wirelessly deployed sensors communicated to and coordinate through a central service, which is accessible by a plurality of users. The locations of these sensors are known to the central service, so that when a sensor generates an alert or other report, the central service can track the various events monitored by the sensors across time and space. By amalgamating the reports from several sensors, the central service can identify trends in events (e.g., a flow of events) to provide one or more users with relevant alerts, reaction plans based on the flow of events, and predictions for

future events in the flow of events. Accordingly, the present disclosure provides an improved user experience and additional functionality for various sensors and the users of those sensors. Additional benefits are provided in the data security of the decentralized reports received by the central service via the use of authentication and blockchain technologies to thereby provide reliable records of past events, and exclude bad actors from submitting false reports through the system. Further benefits and improvements offered by the incident response notification system will be apparent to those of skill in the art on reading the present disclosure

[0015] Although the present disclosure provides several examples of specific hardware, use cases, numbers of elements, terminology, and the like, these are provided to teach/demonstrate a non-limiting subset of the use cases and configurations of the claimed inventions. The examples and aspects disclosed herein are to be construed as merely illustrative and not a limitation of the scope of the present disclosure in any way. It will be apparent to those having skill in the art that changes may be made to the details of the below-described examples without departing from the underlying principles discussed. In other words, various modifications and improvements of the examples specifically disclosed in the description below are within the scope of the appended claims. For instance, any suitable combination of features of the various examples described is contemplated.

[0016] Figure 1 illustrates an operations environment for an incident response notification system 100, according to embodiments of the present disclosure. The operations environment includes various user devices 110 that are associated with users concerned or interested in receiving status updates from various sensors 130 positioned throughout the operations environment, which are in communication with one another via a central service 120. The incident response notification system 100 is developed based on the sensors 130, which communicate with appropriate available Application Programming Interface (API) with the central service 120, which in turn reflects collected and processed incident information on mobile phones, laptops, or other user devices 110 through the Internet.

[0017] The user devices 110 may represent different types of computing devices (as described in greater detail in regard to Figure 6A-6C), which can individually access the central service 120 to receive incident statuses and response plans from the central service 120 based on collected alerts from the sensors 130 and processed knowledge of the operations environment. In various embodiments, the user devices 110 may represent, by way of non-limiting example: mobile phones

of various makes and models, personal computers, laptop computers, slate or tablet devices, smart watches, pagers, or the like.

[0018] The central service 120 acts as a gathering point for alert and status information from the various sensors 130 deployed to an operations environment and access point for those data for the various user devices 110. In various embodiments, the central service 120 may be a centralized, decentralized, or distributed computing environment that includes one or more computing devices (as described in greater detail in regard to Figures 6A-6C). The central service 120 may be accessible to the various user devices 110 and sensors 130 via interface software/logic, application program interfaces (APIs), direct software/logic, publically accessible outputs (e.g., websites, apps), or the like.

[0019] In various embodiments, the central service 120 may include various centralized or decentralized databases, although if block chain technology is used, preferably a distributed database is used, with various hardware/storage layers providers selected for the deployment scenario. In various embodiments, the database may use available products like Oracle/SQL server/MongoDB, and if block chain technology is used an option for public, private, consortium, or hybrid operation is also selected.

[0020] In some embodiments, the central service 120 provides one or more APIs to interface between the user devices 110 (e.g., a web interface 122) and the sensors 130 (e.g., a sensor interface 128) and the various mappings or maps of the status reports from the sensors 130. For example, a sensors interface 128 may receive and reformat status reports from the sensors 130 to incorporate those reports into a format used by a status blockchain 124 or database 126 that is used to generate a map of the environment with the various statuses and reaction plans to those statuses when an incident is identified displayed thereon. This map and other elements of the reaction plan may be accessible to the user devices 110 via the web interface 122, which can be output to applications executing on the various user devices 110 or via a website or app accessible and navigable by a user device 110. In various embodiments, the sensor interface 128 may be used for two-way communication with the sensors 130, to send queries or challenges from the central service 120 to the sensors 130 or to send portions of a reaction plan to the sensors 130. Additionally or alternatively, the central service 120 can use the web interface 122 to communicate with the sensors 130, which may act as user devices 110 for the purpose of receiving reaction plans in

addition to the sensing functionality for reporting environmental conditions and alerts to the central service 120.

[0021] The sensors 130 may represent different types of devices used to detect various conditions in the operations environment and may include, or be in communication with a computing device (as described in more detail in regard to Figure 6A) to report these conditions to the central service 120. In various embodiments, the sensors 130 may represent, by way of non-limiting example: fire alarms, thermostats, motion detectors, Analog & Infrared Sensor, Passive & Active Infrared Sensor, Temperature and proximity sensors, ultrasonic sensors, accelerometers, gyroscopes (e.g., position sensors), pressure sensors, magnetic field sensors (e.g., Hall Effect sensors), proximity sensors, light sensors, smoke/gas/alcohol sensors, touch sensors, color sensors, humidity sensors, or the like. In various embodiments, the sensors 130 are provided as Internet of Things (IoT) devices.

[0022] For example, digital Sensors/Fire Alarms/Thermostats are placed at appropriate or required places in an environment to thereby send alert calls or communicate with the API for the central service 120, which records in a database these alert calls and communications. The collected data are then processed and reflected in website or app according to the need of the user or the application requirements for access by one or more user device 110. Whenever the sensors 130 are triggered, the updated communications are sent to the central service 120, which updates a table of records (e.g., a database), and simultaneously reflects these data in the website or by receiving alert calls and with help of cloud powered voice API integrating into website/app (application).

[0023] In some embodiments, the sensors 130 include voice detection sensors, which include a microphone or other sound collecting device, and logic to process utterances collected from the environment. The logic can include trigger word detection (e.g., scanning for a specific word or phrase before activating speech processing logic), noise filtering, sound level detection, or the like. The sensor 130 can locally process speech detected from the environment, or may transmit audio (compressed, encrypted, truncated, or combinations thereof) to an external service for processing. In various embodiments, the central service 120 includes an API (e.g., the web interface 122 or another interface) to send received utterances to a third-party transcription or speech processing service, or may locally process the voice data for data of interest. These voice alerts can include

information from the environment that are identified by a human that may otherwise be difficult or impossible with the sensors 130 included in the environment.

[0024] In various embodiments, the sensors 130 include various output devices such as lights, speakers, buzzers, sirens, or the like, and combinations thereof to locally output the statuses collected by the sensors 130. For example, a sensor 130 of a smoke detector may include a strobe light and a siren that activate in response to detecting smoke in addition to reporting the detection of smoke to the central service 120. In some embodiments of sensors 130 that include speakers as output devices, the central service 120 can provide cues or voice files to the sensor 130 to output voice instructions to persons located in the environment. For example, in a large building in which a fire has occurred, the central service 120 can provide different voice instructions to different sensors 130 to guide persons in the building to the closest still-available exits.

[0025] Each of the sensors 130 includes a wireless communications device to wireless communicate with the central service 120. Because the various incidents that the sensors 130 are deployed to monitor may affect or disrupt wired communications, the wireless communications device may be included as an alternative or supplemental means of communication with a wired communication device. For example, a sensor 130 of a fire alarm may use wireless communications to continue reporting status information to the central service 120 regarding a detected fire even when a wire used for communications is disrupted. Similarly, to avoid loss of communications when wired power delivery is interrupted, the sensors 130 may include batteries or other power storage devices so that the sensors 130 may continue operations when wired power delivery is interrupted.

[0026] In various embodiments, the sensor 130 may use various wireless communications protocols to communicate with one another (e.g., as part of mesh network) or the central service 120. In various embodiments, the protocols may include, by way of non-limiting example: the IEEE 802.11 family of standards (e.g., WI-FI®, managed by the Wi-Fi Alliance), BLUETOOTH® (managed by the Bluetooth Special Interest Group), radio protocols, cellular communications protocols (e.g., long term evolution (LTE)), or the like. As one of ordinary skill in the art is expected to be familiar with various wireless communications protocols, and understand that these protocols are constantly being updated, the communication protocols used by the sensors 130 to communicate with one another, an intermediary device, or the central service are also contemplated to expand from the written examples, but generally includes local wireless

networking communication protocols (e.g., Wi-Fi), near-field wireless communication protocols (e.g., Bluetooth), and cellular telephony communication protocols (e.g., LTE).

[0027] Figure 2 is a flowchart for an example method 200 of deploying an incident response notification system, according to embodiments of the present disclosure. Method 200 begins at block 210, where an operator places a communication device with a sensor in the environment to monitor. In various embodiments, the operator considers various requirements, regulation, and goals for a project that indicate the locations, categories, and numbers of sensors or instruments to be deployed. The present disclosure contemplates that various projects will have different numbers and types of sensors or instruments deployed to meet the goals for a deployment, and the operator (as a person of ordinary skill in the art) will be able to interpret these goals and requirements to identify the sensors to deploy, and locations to deploy those sensors.

[0028] For example, a local building code may specify that one fire detector is to be deployed in each room of a dwelling and one carbon monoxide detector is to be deployed on each floor of a dwelling. Accordingly, an operator may use the layout of the building, the goals of the project, and the local building code to identify where to locate the various fire detectors, carbon monoxide detectors, and other sensors using ordinary skill and creativity.

[0029] In various embodiments, depending on the availability of different communications channels in the environment, signaling properties in the environment, and distances of the sensors among one another or a central device used to collect/forward communication among the sensors, the operator may select one or more wireless communications standards for the communication device of the sensor to use. For example, the communication device may use one or more of wired communications, Bluetooth, Wi-Fi, radio protocols, LTE, etc.

[0030] At block 220, the operator registers the location and identity of each sensor deployed as per block 210 as part of the incident response notification system with a map/database hosted by a central service. In various embodiments, every sensor has a name or other identifier that is correlated with the location of the sensor in the environment. In various embodiments, the location may be stored as a set of Global Positioning System (GPS) coordinates, layout coordinates (e.g., using a reference frame of a campus, building, or other environment), or other set of coordinates that can identify where the sensors are located in relation to one another and the environment.

[0031] In some embodiments, the registered sensors are associated with a public/private encryption key pair with the central service for encrypting status alerts from the sensors. Because

the status messages may be relatively simple (e.g., a binary alert/no alert, a timestamp, a device identifier, etc. in a known order/format), messages from the various sensors may be vulnerable to spoofing by malicious parties, even if encrypted. Accordingly, in embodiments that use security-sensitive sensors, registering the location and identity of each sensor may include registering a shared secret or other salting mechanism (preferably a mechanism that changes over time) for each sensor to increase the complexity of the status messages when encrypted and thereby reduce the ability for malicious parties to spoof status messages. Accordingly, the central service can evaluate and determine whether to accept or reject a status message to thereby improve data security for any reported statuses; thereby reducing the likelihood and effectiveness of attacks on the central service or individual sensors.

[0032] In addition or alternatively to using a client-server model, the system can use various peer-to-peer (P2P) models. Accordingly, depending on the specifications set for the system, an operator can select various models, such as, but not limited to, those included in Figures 7A and 7B for a hybrid P2P model or a structured P2P model, respectively, according to embodiments of the present disclosure.

[0033] Accordingly, when provided as a distributed system, the various components interact with one another to achieve a shared objective, such as monitoring a cloud of sensors. The system maintains concurrencies in the various distributed components to achieve a shared objective by accounting for the lack of Global Clock and the possibility that independent components can fail independently of one another, such that when a component of one sub-system fails, the entire system does not fail (e.g., in P2P applications). For example, the presently described system can be applied for any architecture which is deployed across different time zones when a distributed application architecture is applied so that, for example when monitoring a border fence spanning across different time zones, or any distributed system in which a failure in one component, will not affect other components.

[0034] In various embodiments of the present system, block chain technologies are used to aid in decentralization while maintaining accountability (e.g., providing trust) in the system due to the immutable and peer-approved aspects offered by block chains, particularly when used with web 3.0 applications.

[0035] In various embodiments of the present system using a P2P or hybrid P2P architecture, the sensors included in user devices 110 (e.g., cell phones) may be incorporated into a mesh with

other sensors 130 deployed in the environment when a user connects that device to the system (e.g., via a web app), to thereby provide additional details on the environment to the system that are localized to the user. In various embodiments, any device having connectivity to a network and a sensor 130 can be integrated into the mesh of sensors 130 used by the present system. Accordingly, the present system may use an Internet of Things (IoT) approach to building a mesh of sensors 130 that are outside of the control of the system, but provide valueable data for the status of the environment. These sensors 130 may go offline and come online outside of the system's control (e.g., due to users connecting/disconnecting devices per user presence/absence in the environment, due to environmental conditions disabling or enabling the associated devices, etc.).

[0036] In various embodiments, registering the location and identity of the sensors creates (at the central service) a blockchain or other immutable record for either the environment (e.g., shared among the several sensors), or for each individual sensor in the environment. Accordingly, as the sensors generate alerts, an immutable record of these alerts is recorded so that reviewers can be assured of the integrity of the data. By knowing the time and order of the status reports, the blockchain or other immutable record can be used to identify improperly timed, duplicate, or otherwise spoofed status reports from legitimate reports; thereby reducing the likelihood and effectiveness of attacks on the central service or individual sensors.

[0037] Additionally, aside from injection or man-in-the-middle attacks, the system may be designed to avoid or combat distributed denial of service (DDOS) attacks by appropriately scaling the servers used in the central service and/or by selecting a "fail to" status appropriate for the environment (e.g., fail to alerting of an incident when service is interrupted, fail to there not being an incident when service is interrupted).

[0038] At block 230, the operator correlates locations of interest to the sensors. In various embodiments, merely knowing the relevant locations of the sensors can be insufficient to generate a response plan to an incident, and the operator therefore correlates additional locational information with the various sensors. For example, knowing that the first through third sensors are located at respective coordinates $X+3$, X , and $X-3$, can identify that the second sensor located at coordinate X is between the first and third sensors. However, by correlating that fire escapes are located at each of the coordinates $X+3$, X , and $X-3$ with the respective sensors, the incident response notification system can identify a closest available fire escape to a user located at location

X-2 and perform other response planning activities that account for the special nature of some locations.

[0039] In another example, the location of interest to a sensor may identify a detection range of the sensor. For example, in a security system a motion detector may be physically located at coordinates (X_0, Y_0) , but is able to detect motion in an area for coordinates in the range of (X_1, Y_1) - (X_2, Y_2) so that a status report of detected motion can be correlated to the coordinates in the detection range.

[0040] Figure 3 is a flowchart for an example method 300 of operating an incident response notification system, according to embodiments of the present disclosure. Method 300 begins at block 310, where a sensor detects an alert condition. In various embodiments, different sensors may be triggered to detect an alert condition in response to different conditions. For example, a first sensor may be configured to generate an alert every n seconds to provide a periodic status signal, while a second sensor may be configured to generate an alert every $2n$ seconds. In another example, a sensor of a smoke detector may be configured to generate an alert in response to particles interrupting a beam of light. The present disclosure contemplates that many different types of sensors with different trigger conditions can be used.

[0041] At block 320, the central service receives a communication from a sensor in response to the detected alert condition from block 310. In various embodiments, the sensors, when triggered, communicate through various available communicate channels, and the communication may be received directly or indirectly (e.g., via one or more intermediary devices) by the central service.

[0042] At block 330, the central service verifies the sender location and identity of communications received per block 320, to identify whether the communication was received from a legitimate sensor and which sensor the communication was received from. In various embodiments, the central service may save all communication from purported sensors (e.g., to log attempted spoofs, either to the record used by the actual sensors or a quarantined record) or may discard communication from sensors that are not verified (e.g., deleting, dropping, or otherwise not storing the communications). In various embodiments, the central service may decrypt the communications, identify whether the communication include a shared secret, challenge the purported sensor, or perform combinations thereof to determine whether the communication has been legitimately received from the sensor. In various embodiments, data received from sensors

are processed through software logic or an API and stored in a database or block of a blockchain for committal.

[0043] At block 340, the central service updates a database mapping of the environment with the alerts from the sensors. The central service may identify where the alert affects the environment based on the registered location of the sensor in the environment or other correlated locations registered with the sensors (e.g., per method 200 discussed in relation to Figure 2). In various embodiments, the database may be output via a two-dimensional or three-dimensional map of the environment so that a user can visualize the alerts and statuses reported from the sensors in space. Depending on the application for the sensors, the database and visualization can provide for monitoring of various systems, building, and environments, such as, but not limited to: drainage networks, water networks, chemical networks, guiding systems, border fences, metros, tunnels, fire incident notification systems, or the like and combinations thereof.

[0044] At block 350, the central service processes pending alerts to identify an incident flow. The “flow” of an incident, as used herein, refers to the progression of an incident over time. For example, the central service may track a fire’s spread over time and the flow of smoke over time by using several readings from different sensors in the environment over time; noting when different sensors are triggered, maintain a triggered status, stop reporting a triggered status, or go offline. Other examples of incident flow include the progression of water, chemicals, persons, animals, or the like throughout or across various points in an environment over a period of time. In some embodiments, the visualization of the incident may include various time-related aspects such as allowing a user to see an animation of the flow of alerts and statuses over time (e.g., to see not only where a fire is present, but how that fire spread over time). In some embodiments, the visualization of the incident flow may include trick-play commands (e.g., fast forward, rewind, speed-up, slow-down, pause, jump) to view the flow in 1:1 timing ratio and flow direction to real time or a different timing ratio or flow direction.

[0045] At block 360, the central service generates a reaction plan, which can include visual representations, voice/sound representations, and combinations thereof.

[0046] For example, when monitoring an incident of livestock escaping an enclosure, the central service may identify the flow of the incident to identify where the livestock escaped from, and how they have traveled since the escape. These data may be provided to a machine learning model or a rules-based model to identify one or more likely paths that the livestock will travel to

in the future (e.g., based on previous escapes, available routes, expected/maximum speeds of the livestock, etc.) to alert responders for where to intercept the livestock and where to repair the enclosure. The reaction plans may be provided to the responders on a map, showing the site for repair and projected heatmaps of likely locations or previous locations where escaping livestock were located. The reaction plan may be provided in conjunction with a visual output of the alerts (e.g., on a shared map showing locations of the livestock via tracking collars, motion detector alerts, etc.).

[0047] In another example, when monitoring an incident of a fire in a building, the central service may identify the flow of the incident to identify still-available evacuation plans. These data may be provided to a machine a machine learning model or a rules-based model to identify likely paths for the continued spread of the fire so that persons are directed away from the current location of the fire and away from the expected locations to which the fire will spread. The reaction plans may be provided to responders or evacuees on a map, showing paths for escape, but may also be provided as an output to one or more devices in the building (e.g., the sensors) to provide audio or visual escape cues. For example, a firefighter or other user in possession of a user device accessing the central service may be provided a visual map of where the fire is currently located and expected to spread in the next *m* minutes, while the sensors in the environment provide audio output (e.g., “proceed to fire escape A”, “come this way”, sequential output of alarm) and/or visual output (e.g., sequential output of light along a pathway of sensors to provide guiding lights towards an exit).

[0048] In various embodiments, when the sensors or other devices in the environment provide sequential output for the reaction plan, the output may be “driving or notifying ” (e.g., seeking to push away from a location) or “guiding” (e.g., seeking to direct towards a location). For example, consider a hallway with sensors located at points *X*+1, *X*+2, *X*+3, a fire located at point *X*, and a fire escape at location *X*+4. When the sensors output a driving sequence of sounds (e.g., to frighten animals away from the fire and towards the fire escape), the sensors located closer to the fire may output an alarm at a greater volume, a longer duration, or combinations thereof than sensors further from the fire. Accordingly, the sensor at point *X*+1 activates louder/longer than the sensor at point *X*+2, which activates louder/longer than the sensor at point *X*+3 to encourage movement towards point *X*+4 and away from point *X*. In contrast, when providing a guiding sequence of sounds (e.g., playback of “escape this way”), the sensors located closer to the fire escape may output the sounds at greater volume than sensors located closer to the fire, more frequently than sensors located

closer to the fire, in a pattern towards the fire escape, or combinations thereof. Accordingly, a sensor at point X+1 may playback at time T₁, the sensor at point X+2 at time T₂, and the sensor at point X+3 at time T₃ (where T₁-T₂-T₃), where the playback is progressively louder closer to point X+4.

[0049] At block 370, the central service provides the map of alerts and/or the reaction plan to a user device in response to receiving a request from the user device. In various embodiments, map of alerts and the reaction plan may be provided in conjunction with one another (e.g., on a shared map showing locations of alerts and how to react to those alerts), or separately from one another. In some embodiments, the outputs are provided via a website hosted by the central service that the user device access through a web browser, or via an API or specific program executing on a user device to receive and interact with the outputs.

[0050] In some embodiments, the central service may push the outputs to one or more devices (e.g., in response to a preference setting requesting pushed alerts/reaction plans) so that a user can request (before an incident is detected) that alerts and reactions plans be provided to one or more devices. For example, the central service may push the reaction plan to one or more sensors in the environment to alert user who do not have user devices otherwise receiving the reaction plan for how to respond to the incident.

[0051] Because the central service continues to receive alerts from the sensors as time progresses, and knows where the various sensors are located in the environment, the central service can update the reaction plan (and the output thereof) as conditions change and the flow of the incident progresses. Accordingly, method 300 may be performed in a loop, with the map or reaction plan (and output thereof) continuously being adjusted as conditions change.

[0052] Figure 4 illustrates a time chart 400 of operating an incident response notification system with a corresponding environment 420, according to embodiments of the present disclosure. As shown, the time chart 400 displays alerts 410a-h (generally or collectively, alerts 410) associated with various sensors 130a-e at different times T₁-T₅. In various embodiments, times T₁-T₅ may be evenly/ constantly distributed (e.g., $\Delta T_x T_{x+1} = \Delta T_y T_{y+1}$) or unevenly/variably distributed (e.g., $\Delta T_x T_{x+1} \neq \Delta T_y T_{y+1}$). For purposes of the present example, each alert 410 relates to a detected presence of water, but other alerts 410 and combinations of multiple types of alerts 410 are contemplated by the present disclosure.

[0053] In the present example, water flows into a culvert, pond, or other depression that is part of a monitored drainage network, as shown by the action arrow 430 in the environment 420. The first sensor 130a identifies the presence of water at times T_1 and T_2 , and ceases to identify the presence of water at times T_3 - T_5 ; indicating that water flowed over the first sensor 130a between times T_1 - T_2 . Similarly, the second sensor 130b identifies no water present at time T_1 , the presence of water at times T_2 - T_4 , and ceases to identify the presence of water at times T_4 - T_5 ; indicating that water flowed over the first sensor 130a between times T_2 - T_3 . The third sensor 130c identifies the presence of water at times T_3 - T_5 ; indicating that water is present in the depression in the environment 420 starting at time T_3 and continuing to (and potentially past) time T_5 .

[0054] Using the collected data from the alerts 410 at the times that the associated sensors 130 generated those alerts, and the known locations (and sensing ranges) of the sensors 130, the systems and methods of the present disclosure can determine a flow of events. In the present example, the direction and duration flow of water into the depression (and potential depth thereof once settled) can be identified from the timing chart 400. Accordingly, by knowing the flow of events (e.g., water into the depression from the first sensor 130a towards the third sensor 130c), the systems and methods of the present disclosure can provide a reaction plan based on those events. For example, an evacuation plan that directs persons to move away from the third sensor 130 in the direction away from the first sensor 130a (where the water is coming from).

[0055] Figure 5 is a flowchart of an example incident response method 500, according to embodiments of the present disclosure. Method 500 begins at block 510 where voice alerts are received from the sensors. In various embodiments, the sensors may be triggered to collect voice alerts in response to detecting a trigger phrase or the sensor activating due to an environmental condition. For example, a personal assistant (such as the ALEXA® smart home apparatus, offered by Amazon Technologies, Inc.) may be configured to begin collecting voice data in response to a user uttering the name of the device, while a voice recorder in a smoke detector may be configured to begin collecting voice data in response to smoke particulates interrupting a beam (e.g., detecting smoke).

[0056] In various embodiments, the central service can directly receive these voice data from the sensors or indirectly receive these data from a third-party transcription service that converts the utterances into words, intents, and meanings on behalf of the sensors. In embodiments that the central service directly received the voice data from the sensors, the central service may locally

process the voice data, or may send the voice data to a third-party transcription service to return processed voice data for the central service to use. Accordingly, method 500 may iterate block 510 one or more times for a given set of voice data.

[0057] At block 520, the central service processes the voice data for inclusion into the database with other status data. In various embodiments, the central service extracts various data points related to metrics tracked by other sensors in the deployment environment (e.g., users stating that there is smoke in the environment when the environment includes smoke detector sensors) or that is not tracked by other sensors in the deployment environment (e.g., users stating that N persons are located in a room that lacks a camera or other sensors to identify a number of persons in the room). In various embodiments, processing the voice data may include extracting key words from the transcript or the utterances that can be used to fill in the data fields of the

[0058] At block 530, the central service generates a reaction plan using the processed voice data and the sensor data. The central service uses the data (voice and sensor) to identify statuses in the environment (e.g., where smoke is located, where persons are located). Various rules-based or machine learning models may be used to identify the status or forecasted status of an incident that can be communicated to the users in addition to or alternatively to a reaction plan. Using the data in the database, the central service generates one or more reaction plans to the incident (e.g., where emergency personnel are directed to, where persons are directed to evacuate towards/away from).

[0059] In various embodiments, the reaction plan can include voice instructions that are sent to designated sensors or user devices, which may include prompts for a user to provide voice data. These voice prompts may be generated by the central service on-the-fly, preloaded in an application executing on the user device or sensor, or generated on behalf of the central service by a third-party voice service. For example, the reaction plan may include one or more devices outputting a voice command requesting anyone in a room to identify themselves, whether anyone in the room is hurt, or to provide other voice alerts that can be used to provide further information relevant to the incident.

[0060] At block 540, the central service outputs the incident status and/or reaction plan generated from the voice data and the other sensor data. In various embodiments, the environmental data related to the incident or the reaction plan is pushed to one or more devices, such as sensors or on-call devices. In various embodiments, the environmental data related to the

incident or the reaction plan is provided to one or more devices in response to a request from such a device, such as a serving a webpage showing the data or plan(s). These outputs may be dispersed via APIs or in published to a website or other publically accessible data format that a user device requests via a web browser, or the like.

[0061] Figure 6A illustrates a computing device 600, as may be used in providing user devices 110, a central service 120, or sensors 130, according to embodiments of the present disclosure. The computing device 600 may include at least one processor 610, a memory 620, and a communication interface 630. Figure 6B-6C illustrate examples of various sensors 640 and input/output devices 650 as maybe included in or in communication with various computing devices, according to embodiments of the present disclosure.

[0062] The processor 610 may be any processing unit capable of performing the operations and procedures described in the present disclosure. In various embodiments, the processor 610 can represent a single processor, multiple processors, a processor with multiple cores, and combinations thereof.

[0063] The memory 620 is an apparatus that may be either volatile or non-volatile memory and may include RAM, flash, cache, disk drives, and other computer readable memory storage devices. Although shown as a single entity, the memory 620 may be divided into different memory storage elements such as RAM and one or more hard disk drives. As used herein, the memory 620 is an example of a device that includes computer-readable storage media, and is not to be interpreted as transmission media or signals per se.

[0064] As shown, the memory 620 includes various instructions that are executable by the processor 610 to provide an operating system 622 to manage various features of the computing device 600 and one or more programs 624 to provide various functionalities to users of the computing device 600, which include one or more of the features and functionalities described in the present disclosure. One of ordinary skill in the relevant art will recognize that different approaches can be taken in selecting or designing a program 624 to perform the operations described herein, including choice of programming language, the operating system 622 used by the computing device 600, and the architecture of the processor 610 and memory 620. Accordingly, the person of ordinary skill in the relevant art will be able to select or design an appropriate program 624 based on the details provided in the present disclosure.

[0065] The communication interface 630 facilitates communications between the computing device 600 and other devices, which may also be computing devices as described in relation to Figure 6A. In various embodiments, the communication interface 630 includes antennas for wireless communications and various wired communication ports. The computing device 600 may also include or be in communication, via the communication interface 630, one or more input devices (e.g., a keyboard, mouse, pen, touch input device, etc.) and one or more output devices (e.g., a display, speakers, a printer, etc.).

[0066] The communication interface 630 may be used to communicate with other devices such as sensors 640, input/output devices 650 (e.g., lights, speakers, sirens), and one or more networks 660 that are organized by various communication standards, which may include one or more public and/or private networks via appropriate network connections via the communication interface 630. Various examples of the sensors 640 and input/output devices 650 that may be integrated with the computing device 600 are shown in Figures 6B-6C. It will also be recognized that software instructions may also be loaded into the memory 620 from an appropriate storage medium or via wired or wireless means using the communications interface 630.

[0067] In particular, Figure 6C illustrates various examples of 5G IoT sensors and LTE-M or NB-IoT sensors. 5G IoT sensors leverage the capabilities of the fifth-generation (5G) cellular network technology for IoT applications. 5G offers faster data rates, lower latency, and increased capacity compared to previous wireless technologies. These sensors are designed to take advantage of the high-speed and low-latency capabilities of 5G networks. 5G IoT sensors enable real-time applications, high-definition video streaming, and ultra-reliable communication in underground or metro environments.

[0068] Some non-limiting examples of 5G IoT sensors that can be used in various applications, including underground or metro environments, include: 1) Environmental Sensors that can monitor air quality, temperature, humidity, and other environmental parameters to ensure safe and comfortable conditions in underground or metro areas; 2) Vibration Sensors that detect and measure vibrations, allowing for monitoring of structural health and detecting potential issues in tunnels or metro infrastructure; 3) Sound Sensors that can be used for noise monitoring in metro stations or tunnels to ensure compliance with noise regulations and identify potential noise-related issues; 4) Surveillance Sensors that provide high-definition video streaming, facilitating real-time monitoring and ensuring the safety of underground or metro areas; 5) Gas Sensors that detect the

presence of hazardous gases, such as carbon monoxide or methane, in underground or metro environments to ensure the safety of workers and passengers; 6) Asset Tracking Sensors that are used to track assets, such as vehicles, equipment, or packages, in an underground or metro setting to improve logistics and ensure efficient operations; 7) Crowd Monitoring Sensors that use video or infrared technology to monitor crowd density and movement in metro stations for security and crowd management purposes; 8) Smart City Sensors that monitor and manage various aspects of urban environments, such as air quality sensors, noise sensors, parking sensors, waste management sensors, and traffic sensors; 9) Industrial IoT Sensors that monitor machinery performance, track inventory, manage supply chain logistics, and optimize energy consumption in industries like manufacturing and logistics; 10) Agricultural IoT Sensors that enhance the capabilities of sensors for soil moisture monitoring, crop health monitoring, livestock tracking and monitoring, weather stations, and automated irrigation systems; 11) Healthcare IoT Sensors that enable remote patient monitoring, wearable health devices, telemedicine applications, advanced medical imaging, and real-time asset tracking in hospitals; and 12) Smart Home Sensors for home security systems, energy management systems, smart appliances, and home automation devices.

[0069] LTE-M (Long-Term Evolution for Machines) Sensors are a cellular IoT technologies that are compatible with 4G and 5G networks. These sensors are specifically designed for IoT applications, and can provide enhanced coverage, longer battery life, and improved device density. There are numerous LTE-M sensors available in the market designed specifically for machine-to-machine communication and IoT applications. Some non-limiting examples of LTE-M sensors that can be used in various applications, include: 1) Environmental Sensors that measure parameters such as temperature, humidity, air quality, noise levels, and light intensity; 2) Asset Tracking Sensors that are used for tracking assets such as vehicles, equipment, or packages, providing real-time location information; 3) Water Quality Sensors that monitor parameters like pH levels, temperature, turbidity, dissolved oxygen, and conductivity to ensure water quality in various applications; 4) Energy Monitoring Sensors that enable energy consumption monitoring for appliances, buildings, or industrial equipment, tracking energy efficiency and identifying areas for optimization; 5) Agriculture Sensors that monitor soil moisture, temperature, humidity, light levels, and rainfall to optimize irrigation, enhance crop health, and improve farm management; 6) Motion Detection Sensors that detect motion or changes in the surrounding environment, enabling applications like security systems, occupancy monitoring, or asset protection; 7) Gas and Chemical

Sensors that detect and measure the concentration of gases and chemicals, including carbon monoxide, carbon dioxide, methane, volatile organic compounds (VOCs), etc.; 8) Industrial Sensors that offer various functionalities such as measuring pressure, vibration, temperature, or detecting faults in machinery to aid machine health monitoring and predictive maintenance; 9) Parking Sensors that monitor parking space occupancy and provide real-time data to optimize parking availability and guide drivers to available spaces; and 10) Smart City Sensors that monitor various aspects of smart cities, including air quality, waste management, parking, water management, and infrastructure monitoring.

[0070] NB-IoT (Narrowband Internet of Things) Sensors are designed for low-power, wide-area (LPWA) applications and can operate on 4G and 5G networks, and are ideal for applications such as smart cities, asset tracking, smart agriculture, and smart metering. There are several NB-IoT sensors available in the market designed for use in Narrowband Internet of Things (NB-IoT) applications. Some non-limiting examples of NB-IoT sensors that can be used in various applications, include: 1) Environmental Sensors that measure parameters such as temperature, humidity, air quality, noise levels, and light intensity; 2) Asset Tracking Sensors that are used for tracking assets such as vehicles, equipment, or packages, providing real-time location information; 3) Water Quality Sensors that monitor parameters like pH levels, temperature, turbidity, dissolved oxygen, and conductivity to ensure water quality in various applications; 4) Energy Monitoring Sensors that enable energy consumption monitoring for appliances, buildings, or industrial equipment, tracking energy efficiency and identifying areas for optimization; 5) Agriculture Sensors that monitor soil moisture, temperature, humidity, light levels, and rainfall to optimize irrigation, enhance crop health, and improve farm management; 6) Motion Detection Sensors that detect motion or changes in the surrounding environment, enabling applications like security systems, occupancy monitoring, or asset protection; 7) Gas and Chemical Sensors that detect and measure the concentration of gases and chemicals, including carbon monoxide, carbon dioxide, methane, volatile organic compounds (VOCs), etc.; 8) Industrial Sensors that offer various functionalities such as measuring pressure, vibration, temperature, or detecting faults in machinery to aid machine health monitoring and predictive maintenance; 9) Parking Sensors that monitor parking space occupancy and provide real-time data to optimize parking availability and guide drivers to available spaces; and 10) Smart City Sensors that monitor various aspects of smart cities,

including air quality, waste management, parking, water management, and infrastructure monitoring.

[0071] Accordingly, the computing device 600 is an example of a system that includes a processor 610 and a memory 620 that includes instructions that (when executed by the processor 610) perform various embodiments of the present disclosure. Similarly, the memory 620 is an apparatus that includes instructions that when executed by a processor 610 perform various embodiments of the present disclosure.

[0072] The present disclosure may also be understood with reference to the following example of applying the present disclosure to a multistoried building to monitor for fires. When a fire breaks out on floor, for example, 20th floor, users on different floors are given different evacuation instructions. Users on lower floors (e.g., floors 19 and below) are directed to the closest fire escapes, but users located on higher floors can be directed to a subset of the available fire escapes, which may not necessarily be the closest fire escape on a given floor. Accordingly, the present disclosure directs these persons to the fire escapes with the least smoke, least risk of fire spreading to block the particular fire escape, fewest number of evacuees (e.g., to allow for faster evacuation and avoid bottlenecks), or otherwise improved ability to safely exit the multistoried building.

[0073] In this example, each floor and in each room/office/apartment thereof, the system includes various sensors (e.g., fire alarms, thermostats, smoke detectors, motion sensors, carbon monoxide detectors, etc.), which include cellular communication devices with N (e.g., five) preinstalled telephone numbers. These cellular communication devices may be add-ons or integrated with the sensors, and are configured via onboard logic to auto dial and send messages to the central service when an associated sensors is triggered. The various sensors may be placed according to local building codes, and in the present example include thermostat sensors placed in the stairwells at every location, with a fixing temperature limit F (e.g., $F=70$ degrees Celsius) to trigger when a stairwell is “hot” and is dangerous to use as an evacuation route. These stairwell readings can be augmented by the alerts generated by smoke detectors, carbon monoxide detectors, thermostats, etc. located on the various floors of a building to identify when a fire is approaching or near the stairwell, and may make the stairwell unsafe to use as an escape route (now or in the future). Additionally, voice calls received from user devices or audio identified by the sensors when triggered can be sent to the central service (e.g., directly or via a third-part transcription service) to identify further pertinent data from users located in the environment

[0074] These data are collected and processed via the central service, which may provide various outputs to different users and different devices. For example, a first web page comprised of headings in the order of receipt the various sensors can be provided to show the spread of the fire to evacuees or firefighters. In other web pages, different floors of the building can be shown individually, or collectively, with overlays of where and when the different status reports were received, a predicted incident flow for the fire, and/or evacuation routes and other response plans in reaction to the fire. These outputs can include maps that indicate the stairwells, temperatures, smoke content, air quality, number of persons in a given area, or the like.

[0075] Each floor in a web page can be divided into various text boxes that are sized and arranged to mimic the building. For example, a rectangular building may with stairwells located on either end of the rectangle can be represented by three boxes placed in a row for a first stairwell, a central living/apartment/office area, and a third stairwell, respectively. Text boxes can be shown with green and red colors; whenever any staircase/fire alarms are triggered, textbox changes color to red otherwise it is green to clearly differentiate safe and potentially dangerous escape routes. Additionally, various textual notes can be included in the text box indicating how many persons are located on each floor, when an alarm triggered, a current temperature, or the like. As the text and color of the various boxes require less overhead to transmit than graphical maps, the central service can reduce the amount of data transmitted among the various devices to accurately represent the state of the incident to prior solutions, while still presented an easy to read interface to multiple devices.

[0076] In addition to the embodiments described above, many examples of specific combinations are within the scope of the disclosure, some of which are detailed below:

[0077] Clause 1: A method, comprising: receiving, at a central service from a wireless communication device associated with a sensor deployed in an environment with a plurality of sensors, a status report; verifying, by the central service, a location of the sensor in the environment; updating, by the central service, a map of the environment with the status report; processing, by the central service, pending status reports, including the status report, to identify an incident flow; generating, by the central service, a reaction plan based on the map and the incident flow; and outputting, via the central service, the reaction plan.

[0078] Clause 2: The method of any of clauses 1 or 3-10, further comprising: verifying, by the central service, an identify of the sensor before updating the map of the environment with the status report.

[0079] Clause 3: The method of any of clauses 1-2 or 4-10, further comprising: receiving, at the central service from a second wireless communication device associated with a second sensor deployed in the environment with the plurality of sensors, a second status report; verifying, by the central service, a second location of the second sensor in the environment; updating, by the central service, the map of the environment with the second status report; and wherein processing, by the central service, the pending status reports to identify the incident flow, further includes the second status report.

[0080] Clause 4: The method of any of clauses 1-3 or 4-10, wherein the map of the environment is maintained via a blockchain including previously submitted status reports.

[0081] Clause 5: The method of any of clauses 1-4 or 6-10, wherein processing, by the central service, the status report to identify the incident flow includes extracting voice data from the status report.

[0082] Clause 6: The method of any of clauses 1-5 or 7-10, wherein the reaction plan is accessible via a website or app hosted by the central service.

[0083] Clause 7: The method of any of clauses 1-6 or 8-10, wherein the central service outputs the reaction plan via the plurality of sensors.

[0084] Clause 8: The method of any of clauses 1-7 or 9-10, wherein the central service includes a first application program interface (API) that interfaces between the plurality of sensors and a database providing the map of the environment or a blockchain providing the map of the environment, and a second API that interfaces between the map of the environment and a plurality of user devices.

[0085] Clause 9: The method of any of clauses 1-8 or 10, wherein the plurality of sensors include one or more types of sensors including one or more of: fire alarms, thermostats, motion detectors, proximity sensors, ultrasonic sensors, accelerometers, gyroscopes, pressure sensors, Hall Effect sensors, light sensors, smoke/gas/alcohol sensors, touch sensors, color sensors, humidity sensors; a fifth generation (5G) Internet of Thing (IOT) sensor including at least one of: environmental sensors, asset tracking sensors, sound sensors, surveillance sensors, gas sensors, vibration sensors, crowd monitoring sensors, smart city sensors, industrial IOT sensors,

agricultural IOT sensors, healthcare IOT sensors, and smart home sensors; and a long term evolution (LTE) sensor or a Narrow Band (NB) IOT sensor including at least one of: environmental sensors, asset tracking sensors, water quality sensors, energy monitoring sensors, agriculture sensors, motion detection sensors, gas and chemical sensors, industrial sensors, parking sensors, and smart city sensors.

[0086] Clause 10: The method of any of clauses 1-9, wherein the wireless communication device communicates with the central service using a wireless communication protocol selected from the group consisting of: Wi-Fi; Bluetooth; Cellular telephony networking; and Radio protocols.

[0087] Clause 11: A system, comprising: a processor; and a memory including instructions, that when executed by the processor perform operations comprising: receiving, at a central service from a wireless communication device associated with a sensor deployed in an environment with a plurality of sensors, a status report; verifying, by the central service, a location of the sensor in the environment; updating, by the central service, a map of the environment with the status report; processing, by the central service, pending status reports, including the status report, to identify an incident flow; generating, by the central service, a reaction plan based on the map and the incident flow; and outputting, via the central service, the reaction plan.

[0088] Clause 12: The system of any of clauses 11 and 13-17, the operations further comprising: verifying, by the central service, an identify of the sensor before updating the map of the environment with the status report.

[0089] Clause 13: The system of any of clauses 11-12 and 14-17, the operations further comprising: receiving, at the central service from a second wireless communication device associated with a second sensor deployed in the environment with the plurality of sensors, a second status report; verifying, by the central service, a second location of the second sensor in the environment; updating, by the central service, the map of the environment with the second status report; and wherein processing, by the central service, the pending status reports to identify the incident flow, further includes the second status report.

[0090] Clause 14: The system of any of clauses 11-13 and 15-17, wherein the map of the environment is maintained via a blockchain including previously submitted status reports.

[0091] Clause 15: The system of any of clauses 11-14 and 16-17, wherein processing, by the central service, the status report to identify the incident flow includes extracting voice data from the status report.

[0092] Clause 16: The system of any of clauses 11-15 and 17, wherein the reaction plan is accessible via a website hosted by the central service.

[0093] Clause 17: The system of any of clauses 11-16, wherein the central service outputs the reaction plan via the plurality of sensors.

[0094] Clause 18: A system, comprising: a sensor; an output device; a processor; and a memory including instructions, that when executed by the processor perform operations comprising: in response to detecting a triggering condition via the sensor, wirelessly transmitting a status report to a central service in communication with the sensor and a plurality of other sensors in an environment with the system; receiving, from the central service, an incident response plan that indicates a series of actions for the output device to perform in tandem with one or more other output devices of the plurality of other sensors; and outputting the incident response plan via the output device.

[0095] Clause 19: The system of any of claims 18 and 20, wherein the incident response plan includes voice commands for users located in the environment.

[0096] Clause 20: The system of any of claims 18-19, wherein the incident response plan includes at least one of: a sequential sound pattern of a driving sound or a guiding sound to be performed based on relative locations of the sensor and the plurality of other sensors in the environment and an evacuation route mapped through the environment; or a sequential light pattern of a guiding light to be performed based on relative locations of the sensor and the plurality of other sensors in the environment and an evacuation route mapped through the environment.

[0097] Certain terms are used throughout the description and claims to refer to particular features or components. As one skilled in the art will appreciate, different persons may refer to the same feature or component by different names. This document does not intend to distinguish between components or features that differ in name but not function.

[0098] As used herein, “about,” “approximately” and “substantially” are understood to refer to numbers in a range of the referenced number, for example the range of -10% to +10% of the referenced number, preferably -5% to +5% of the referenced number, more preferably -1% to +1% of the referenced number, most preferably -0.1% to +0.1% of the referenced number.

[0099] Furthermore, all numerical ranges herein should be understood to include all integers, whole numbers, or fractions, within the range. Moreover, these numerical ranges should be construed as providing support for a claim directed to any number or subset of numbers in that range. For example, a disclosure of from 1 to 10 should be construed as supporting a range of from 1 to 8, from 3 to 7, from 1 to 9, from 3.6 to 4.6, from 3.5 to 9.9, and so forth.

[00100] As used in the present disclosure, a phrase referring to “at least one of” a list of items refers to any set of those items, including sets with a single member, and every potential combination thereof. For example, when referencing “at least one of A, B, or C” or “at least one of A, B, and C”, the phrase is intended to cover the sets of: A, B, C, A-B, B-C, and A-B-C, where the sets may include one or multiple instances of a given member (e.g., A-A, A-A-A, A-A-B, A-A-B-B-C-C-C, etc.) and any ordering thereof. For avoidance of doubt, the phrase “at least one of A, B, and C” shall not be interpreted to mean “at least one of A, at least one of B, and at least one of C”.

[00101] As used in the present disclosure, the term “determining” encompasses a variety of actions that may include calculating, computing, processing, deriving, investigating, looking up (e.g., via a table, database, or other data structure), ascertaining, receiving (e.g., receiving information), accessing (e.g., accessing data in a memory), retrieving, resolving, selecting, choosing, establishing, and the like.

[00102] Without further elaboration, it is believed that one skilled in the art can use the preceding description to use the claimed inventions to their fullest extent. The examples and aspects disclosed herein are to be construed as merely illustrative and not a limitation of the scope of the present disclosure in any way. It will be apparent to those having skill in the art that changes may be made to the details of the above-described examples without departing from the underlying principles discussed. In other words, various modifications and improvements of the examples specifically disclosed in the description above are within the scope of the appended claims. For instance, any suitable combination of features of the various examples described is contemplated.

[00103] Within the claims, reference to an element in the singular is not intended to mean “one and only one” unless specifically stated as such, but rather as “one or more” or “at least one”. Unless specifically stated otherwise, the term “some” refers to one or more. No claim element is to be construed under the provision of 35 U.S.C. § 112(f) unless the element is expressly recited using the phrase “means for” or “step for”. All structural and functional equivalents to the elements

of the various embodiments described in the present disclosure that are known or come later to be known to those of ordinary skill in the relevant art are expressly incorporated herein by reference and are intended to be encompassed by the claims. Moreover, nothing disclosed in the present disclosure is intended to be dedicated to the public regardless of whether such disclosure is explicitly recited in the claims.

CLAIMS

The invention is claimed as follows:

1. A method, comprising:
receiving, at a central service from a wireless communication device associated with a sensor deployed in an environment with a plurality of sensors, a status report;
verifying, by the central service, a location of the sensor in the environment;
updating, by the central service, a map of the environment with the status report;
processing, by the central service, pending status reports, including the status report, to identify an incident flow;
generating, by the central service, a reaction plan based on the map and the incident flow;
and
outputting, via the central service, the reaction plan.
2. The method of claim 1, further comprising:
verifying, by the central service, an identify of the sensor before updating the map of the environment with the status report.
3. The method of claim 1, further comprising:
receiving, at the central service from a second wireless communication device associated with a second sensor deployed in the environment with the plurality of sensors, a second status report;

verifying, by the central service, a second location of the second sensor in the environment;

updating, by the central service, the map of the environment with the second status report; and

wherein processing, by the central service, the pending status reports to identify the incident flow, further includes the second status report.

4. The method of claim 1, wherein the map of the environment is maintained via a blockchain including previously submitted status reports.

5. The method of claim 1, wherein processing, by the central service, the status report to identify the incident flow includes extracting voice data from the status report.

6. The method of claim 1, wherein the reaction plan is accessible via a website or app hosted by the central service.

7. The method of claim 1, wherein the central service outputs the reaction plan via the plurality of sensors.

8. The method of claim 1, wherein the central service includes a first application program interface (API) that interfaces between the plurality of sensors and a database providing the map of the environment or a blockchain providing the map of the environment, and a second API that interfaces between the map of the environment and a plurality of user devices.

9. The method of claim 1, wherein the plurality of sensors include one or more types of sensors including one or more of:

fire alarms, thermostats, motion detectors, proximity sensors, ultrasonic sensors, pressure sensors, Hall Effect sensors, light sensors, smoke/gas/alcohol sensors, touch sensors, color sensors, humidity sensors;

a fifth generation (5G) Internet of Thing (IOT) sensor including at least one of:

environmental sensors, asset tracking sensors, sound sensors, surveillance sensors, gas sensors, vibration sensors, crowd monitoring sensors, smart city sensors, industrial IOT sensors, agricultural IOT sensors, healthcare IOT sensors, and smart home sensors;
and

a long term evolution (LTE) sensor or a Narrow Band (NB) IOT sensor including at least one of:

environmental sensors, asset tracking sensors, water quality sensors, energy monitoring sensors, agriculture sensors, motion detection sensors, gas and chemical sensors, industrial sensors, parking sensors, and smart city sensors.

10. The method of claim 1, wherein the wireless communication device communicates with the central service using a wireless communication protocol selected from the group consisting of:

Wi-Fi;

Bluetooth;

Cellular telephony networking; and

Radio protocols.

11. A system, comprising:
 - a processor; and
 - a memory including instructions, that when executed by the processor perform operations comprising:
 - receiving, at a central service from a wireless communication device associated with a sensor deployed in an environment with a plurality of sensors, a status report;
 - verifying, by the central service, a location of the sensor in the environment;
 - updating, by the central service, a map of the environment with the status report;
 - processing, by the central service, pending status reports, including the status report, to identify an incident flow;
 - generating, by the central service, a reaction plan based on the map and the incident flow;
 - and
 - outputting, via the central service, the reaction plan.
12. The system of claim 11, the operations further comprising:
 - verifying, by the central service, an identify of the sensor before updating the map of the environment with the status report.
13. The system of claim 11, the operations further comprising:

receiving, at the central service from a second wireless communication device associated with a second sensor deployed in the environment with the plurality of sensors, a second status report;

verifying, by the central service, a second location of the second sensor in the environment;

updating, by the central service, the map of the environment with the second status report; and

wherein processing, by the central service, the pending status reports to identify the incident flow, further includes the second status report.

14. The system of claim 11, wherein the map of the environment is maintained via a blockchain including previously submitted status reports.

15. The system of claim 11, wherein processing, by the central service, the status report to identify the incident flow includes extracting voice data from the status report.

16. The system of claim 11, wherein the reaction plan is accessible via a website hosted by the central service.

17. The system of claim 11, wherein the central service outputs the reaction plan via the plurality of sensors.

18. A system, comprising:

a sensor;
an output device;
a processor; and
a memory including instructions, that when executed by the processor perform operations comprising:

in response to detecting a triggering condition via the sensor, wirelessly transmitting a status report to a central service in communication with the sensor and a plurality of other sensors in an environment with the system;

receiving, from the central service, an incident response plan that indicates a series of actions for the output device to perform in tandem with one or more other output devices of the plurality of other sensors; and

outputting the incident response plan via the output device.

19. The system of claim 18, wherein the incident response plan includes voice commands for users located in the environment.

20. The system of claim 18, wherein the incident response plan includes at least one of:

a sequential sound pattern of a driving sound or a guiding sound to be performed based on relative locations of the sensor and the plurality of other sensors in the environment and an evacuation route mapped through the environment; or

a sequential light pattern of a guiding light to be performed based on relative locations of the sensor and the plurality of other sensors in the environment and an evacuation route mapped through the environment.